Nattan MAISONNEUVE–FLEURY
BTS SIO 1
Groupe B

26/11/2025

Compte Rendu - Atelier 10 : TP2 Sécurité informatique

Sommaire :

Introduction :

Dans ce TP, nous allons voir comment récupérer des informations et travailler en équipe afin de sécuriser un espace de travail.

Phase 1 - Analyse et préparation :

Annexes 1 :

Le CNRS a appliquer 5 principes fondamentaux de la sécurité dans le contexte du laboratoire pharmaceutique Galaxy Swiss Bourdin (GSB) :

- Confidentialité (les informations sont géré et sécurisé)
- Intégrité (assurer que les données ne sont pas modifiées de manière non autorisée)
- Disponibilité (garantir l'accès aux informations et systèmes quand nécessaire)
- Traçabilité (pouvoir retracer toutes les actions sur le système d'information)
- Preuve (pouvoir prouver les actions et leur légitimité)

Dans ce domaine nous avons plusieurs risques principaux identifiés :

Risque	Impact	Probabilité	Mesures de Protection
Perte de données de recherche	Très élevé	Élevée	Sauvegardes régulières, chiffrement
Vol de propriété intellectuelle	Très élevé	Moyenne	Contrôle d'accès strict, monitoring
Intrusion via périphériques USB	Élevé	Élevée	Politique d'usage, antivirus, contrôle
Erreur humaine	Élevé	Élevée	Formation, procédures, double validation
Panne système	Élevé	Faible	Redondance, plan de reprise

Et aussi des mesures de protections :

✅ **Checklist des Bonnes Pratiques GSB**

✓ **Authentification Forte**
Mots de passe complexes + double authentification pour les accès sensibles

✓ **Contrôle des Périphériques USB**
Autorisation préalable obligatoire + chiffrement des données

✓ **Sauvegardes Régulières**
Sauvegardes quotidiennes avec test de restauration mensuel

✓ **Mises à Jour de Sécurité**
Application systématique des correctifs dans les 48h

✓ **Formation des Utilisateurs**
Formation obligatoire annuelle sur la sécurité informatique

✓ **Monitoring Continu**
Surveillance 24/7 des systèmes critiques et détection d'intrusion

5 étapes sont importantes à faire immédiatement en cas de procédure d'urgence :

1. **Isoler** le système compromis du réseau
2. **Alerter** le responsable sécurité et la direction
3. **Documenter** tous les détails de l'incident
4. **Préserver** les preuves pour investigation
5. **Appliquer** le plan de reprise d'activité

Annexes 2 :

Sujet : Analyse des cybermenaces contemporaines (basée sur les 15 premières minutes du documentaire d'Arte).

Points Clés du Documentaire

Analyse de la nature des menaces actuelles.

Guerre asymétrique : Les conflits cybernétiques sont présentés comme une nouvelle forme de guerre où États et criminels utilisent Internet comme champ de bataille.

Attaques d'infrastructures : Des systèmes vitaux peuvent être paralysés sans qu'il soit nécessaire d'utiliser la force physique traditionnelle.

Problème d'attribution : Il est très difficile d'identifier formellement les auteurs, ce qui crée un "déni plausible" stratégique pour les attaquants.

Économie souterraine : Il existe des marchés parallèles florissants pour l'achat de vulnérabilités "zero-day" et de services de piratage.

Vulnérabilité des entreprises : Même les entreprises bien protégées sont infiltrées facilement via l'ingénierie sociale ou les failles humaines.

Enjeux Identifiés pour GSB

Risques spécifiques au contexte pharmaceutique.

Vol de Propriété Intellectuelle : Les données de recherche sont une cible privilégiée pour les cybercriminels.

Espionnage Industriel : Les brevets (formules) et les résultats d'essais cliniques sont particulièrement vulnérables.

Attaques Ciblées : En tant que leader du marché, GSB risque de subir des attaques sophistiquées.

Facteur Humain : Les employés et chercheurs constituent le "premier maillon faible" de la chaîne de sécurité.

Recommandations pour GSB

Mesures de protection inspirées du documentaire.

Formation Continue : Sensibilisation obligatoire à l'ingénierie sociale et au phishing.

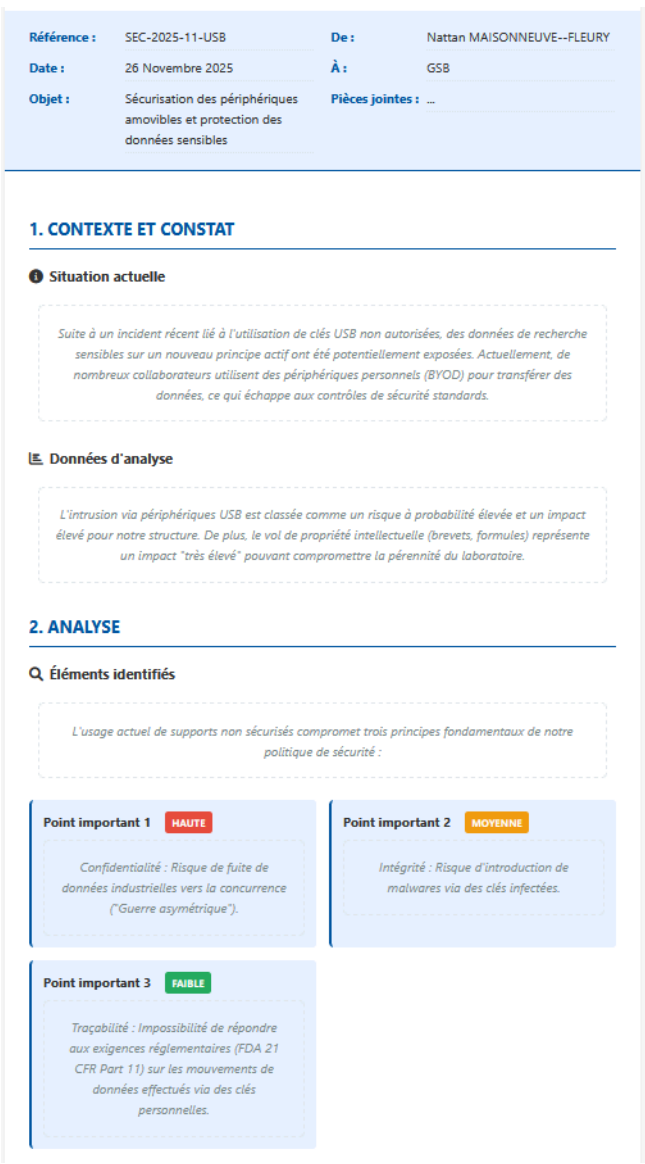
Surveillance Proactive : Mise en place de détection d'intrusion avancée et monitoring 24/7.

Protection des Données : Chiffrement systématique des données de recherche et application du principe de moindre privilège.

Plan de Réponse : Procédures claires pour isoler les systèmes et préserver les preuves en cas d'incident.

Collaboration : Participation aux groupes de partage d'informations sur les menaces du secteur.

Phase 2 - Rédaction et validation :



Référence :	SEC-2025-11-USB	**De :**	Nattan MAISONNEUVE--FLEURY
Date :	26 Novembre 2025	**À :**	GSB
Objet :	Sécurisation des périphériques amovibles et protection des données sensibles	**Pièces jointes :**	...

1. CONTEXTE ET CONSTAT

Situation actuelle

Suite à un incident récent lié à l'utilisation de clés USB non autorisées, des données de recherche sensibles sur un nouveau principe actif ont été potentiellement exposées. Actuellement, de nombreux collaborateurs utilisent des périphériques personnels (BYOD) pour transférer des données, ce qui échappe aux contrôles de sécurité standards.

Données d'analyse

L'intrusion via périphériques USB est classée comme un risque à probabilité élevée et un impact élevé pour notre structure. De plus, le vol de propriété intellectuelle (brevets, formules) représente un impact "très élevé" pouvant compromettre la pérennité du laboratoire.

2. ANALYSE

Éléments identifiés

L'usage actuel de supports non sécurisés compromet trois principes fondamentaux de notre politique de sécurité :

Point important 1 HAUTE

Confidentialité : Risque de fuite de données industrielles vers la concurrence ("Guerre asymétrique").

Point important 2 MOYENNE

Intégrité : Risque d'introduction de malwares via des clés infectées.

Point important 3 FAIBLE

Traçabilité : Impossibilité de répondre aux exigences réglementaires (FDA 21 CFR Part 11) sur les mouvements de données effectués via des clés personnelles.

3. RECOMMANDATIONS

Propositions d'action

Présenter les recommandations générales et objectifs...

Plan d'action proposé

Action prioritaire 1

Responsable: ... Échéance: ... HAUTE

Interdiction formelle de l'usage de clés USB personnelles (modification de l'article 4 de la Charte Informatique).

Action prioritaire 2

Responsable: ... Échéance: ... MOYENNE

Dotation exclusive en clés USB d'entreprise chiffrées matériellement pour les collaborateurs ayant un besoin justifié.

Action complémentaire

Responsable: ... Échéance: ... FAIBLE

Mise en place de stations de désinfection antivirale obligatoires avant toute connexion d'un périphérique externe.

4. CONCLUSION

La mise en œuvre stricte de cette nouvelle politique USB garantira la confidentialité de nos brevets et l'intégrité des résultats d'essais cliniques, actifs vitaux pour GSB. En remplaçant l'usage de périphériques personnels par des solutions d'entreprise chiffrées, nous assurons non seulement la traçabilité exigée par les normes FDA 21 CFR Part 11 et EMA, mais nous réduisons également drastiquement la surface d'attaque face aux risques d'espionnage industriel et d'intrusion virale.

Nous recommandons la validation de l'achat de supports chiffrés et la modification immédiate de la Charte Informatique (articles 4 et 5) pour interdire les clés personnelles. Ce déploiement technique doit être accompagné d'une campagne de sensibilisation auprès des équipes R&D pour renforcer la vigilance humaine.

Pour le service émetteur

MAISONNEUVE--FLEURY Nattan

Vu et approuvé

CONFIDENTIEL - Usage interne GSB uniquement

Page 1/1

Phase 3 - Communication et formation :

Questions de Préparation

Quels sont les 3 arguments principaux que vous utiliserez pour convaincre le comité de l'urgence des mesures ?

- **Protection du Secret Industriel :** Une fuite de brevet ou de formule tue notre avantage concurrentiel.
- **Conformité FDA/EMA :** Les clés personnelles non tracées nous mettent dans l'illégalité (risque d'amendes/perte de certification).
- **Continuité de Service :** Une clé infectée peut arrêter toute l'usine. Le coût de la sécurité est dérisoire comparé à un arrêt de production.

Comment allez-vous présenter l'incident récent sans créer de panique mais en montrant la gravité ?

Ne pas paniquer, mais responsabiliser : "C'est un incident *maîtrisé* qui agit comme un signal d'alarme. Nos portes sont blindées, mais nos fenêtres (ports USB) sont ouvertes.".

Quelles objections anticipez-vous de chaque directeur et comment y répondrez-vous ?

- **À la Recherche (Peur des lenteurs) :** "Perdre vos données ralentirait le projet bien plus qu'une procédure de sécurité. Nous allons vous équiper de matériel rapide.".
- **Aux Opérations (Peur des contraintes) :** "Intégration fluide dans les sas existants avec des stations de décontamination dédiées.".

Phase 4 - Synthèse et évaluation :

Chers collaborateurs,

Suite à l'audit de sécurité et dans le cadre de notre engagement continu à protéger nos données sensibles (propriété intellectuelle, données patients et résultats de recherche), une nouvelle politique de sécurité informatique renforcée va être déployée.

Ce qui change :

1. **Nouveaux équipements :** Nous allons procéder au déploiement progressif de 450 nouveaux ordinateurs portables intégrant des mesures de sécurité de pointe (chiffrement intégral, TPM, authentification forte).
2. **Règles de sécurité :** De nouvelles directives, détaillées dans la mise à jour de la charte informatique, concernent notamment la gestion des mots de passe, le travail à distance sécurisé, et la vigilance face aux menaces (phishing, ingénierie sociale).
3. **Formation :** Des sessions de sensibilisation obligatoires sur les cybermenaces (conformément aux enjeux d'espionnage industriel) seront planifiées pour tous les personnels.

Votre action immédiate est requise :

- Veuillez prendre connaissance de la **note de service** et de la **mise à jour de la charte informatique** (disponibles sur l'intranet de GSB).
- Soyez attentifs aux communications de la DSI concernant le planning de remplacement de votre poste de travail.

La sécurité de GSB est l'affaire de tous. Merci de votre coopération pour assurer l'intégrité et la confidentialité de nos travaux.

Cordialement,

Le Responsable de la Sécurité des Systèmes d'Information (RSSI)
Galaxy Swiss Bourdin (GSB)
)

Axe de Modification	Modification/Ajout Proposé	Justification Sécurité
Authentification	Passage à l'authentification multi-facteurs (MFA) obligatoire pour l'accès aux ressources critiques (VPN, serveurs de recherche, données RH).	Réduction drastique du risque lié aux mots de passe volés ou faibles et à l'ingénierie sociale.
Protection des Données	Chiffrement intégral (BitLocker ou équivalent) obligatoire sur tous les ordinateurs portables GSB (y compris les 450 nouveaux postes).	Garantir la confidentialité des données de recherche et de la PI en cas de perte ou de vol de l'équipement.
Télé-travail/Accès Distant	Accès distant exclusivement via VPN sécurisé, avec interdiction stricte de stockage de données sensibles en local sur un poste non GSB.	Sécuriser la connectivité et garantir la traçabilité des accès aux ressources GSB.
Ingénierie Sociale	Ajout d'une clause de formation annuelle obligatoire sur le phishing et l'ingénierie sociale (basée sur le "facteur humain" identifié comme vulnérabilité).	Renforcer le "premier maillon faible" de la chaîne de sécurité (les utilisateurs).
Gestion des Incidents	Définition claire de la procédure d'urgence (Isoler, Alerter, Documenter, Préserver, Appliquer le PRA) que tout employé doit suivre.	Assurer une réponse rapide et conforme aux exigences légales et de preuve.

Objectif : Déployer les 450 postes de travail neufs en minimisant l'impact sur les activités métiers critiques.

Phase	Population Ciblée / Sites	Durée Estimée
Phase 1 : Pilote & Sites Sensibles	DSI, R&D (sites de Lyon et Strasbourg), Direction (50 postes)	4 semaines
Phase 2 : Fonctions Support	RH, Finance, Marketing, Commercial (sites de Paris et Bordeaux) (150 postes)	6 semaines
Phase 3 : Force de Vente & Terrain	Visiteurs Médicaux et équipes mobiles (200 postes)	8 semaines
Phase 4 : Achèvement & Réserves	Équipes restantes et stocks de remplacement (50 postes)	4 semaines

Approche : Déploiement par site et par vagues, incluant une mini-formation à la prise en main des nouveaux outils de sécurité (BitLocker, MFA) pour chaque utilisateur.

Critère d'Évaluation	Niveau (Échelle de 1 à 5, 5 étant Excellent)	Points Forts de la Séance
Compréhension des Enjeux	4	Bonne assimilation des principes CNIL/CNRS et des menaces contemporaines (guerre asymétrique, espionnage industriel).
Qualité des Propositions Techniques	3	Définition claire des exigences matérielles (TPM, SSD, chiffrement) et logicielles (MDM, VPN).
Adéquation Métier/Sécurité	4	Les recommandations tiennent compte du besoin de mobilité et de gestion des frais des VM tout en sécurisant la PI.

Critère d'Évaluation	Niveau (Échelle de 1 à 5, 5 étant Excellent)	Points Forts de la Séance
Organisation et Livrables	5	Le compte rendu est structuré, complet et les livrables (charte, email, plan) sont opérationnels.

Dans l'industrie pharmaceutique comme GSB, l'articulation entre sécurité et besoins métiers est un équilibre constant entre la **protection de la Propriété Intellectuelle (PI)** et la **nécessité d'innover rapidement**.

- **Sécurité comme Facilitateur :** La sécurité ne doit pas être perçue comme un frein, mais comme la garantie permettant aux chercheurs et aux commerciaux de travailler avec confiance. Par exemple, le chiffrement intégral permet aux visiteurs médicaux de se déplacer en toute légalité sans craindre la perte de données patient confidentielles.
- **Contrainte et Conformité :** Les exigences réglementaires (CNIL/RGPD pour les données patients, nécessité de "preuve" pour les essais cliniques) imposent des contraintes. Le défi est d'intégrer ces contraintes de manière fluide (ex: MFA non intrusif, VPN rapide) pour maintenir la productivité.
- **Le Cas de la R&D :** Le besoin de collaboration rapide et d'accès aux données de recherche doit être sécurisé sans complexifier le partage. L'utilisation du principe de **moindre privilège** garantit que les chercheurs n'accèdent qu'aux données strictement nécessaires, protégeant ainsi l'ensemble du patrimoine de PI de l'entreprise contre l'espionnage industriel.

Conclusion :

Ce TP a permis d'appliquer les principes de sécurité (C-I-D-T-P) au cas concret de GSB, entreprise pharmaceutique sensible. Nous avons formalisé une politique de sécurité renforcée (MFA, chiffrement) et un plan de déploiement pour protéger l'entreprise contre le vol de propriété intellectuelle. Ce travail a confirmé que la sécurité informatique est un facilitateur d'affaires, essentiel pour l'innovation et la conformité, tout en trouvant l'équilibre avec la productivité des équipes.